



CALIFORNIA OFFICE OF
INFORMATION SECURITY
& PRIVACY PROTECTION



Policy Project Overview

ISO Meeting
March 12, 2009



Introductions

□ Presenters

■ Russell Jones

- rujones@deloitte.com
- 415-783-5054

■ Ravi Inthiran

- rinthiran@deloitte.com
- 415-783-4668

■ Robert Vaile

- rvaile@deloitte.com
- 415-783-6842

■ Ron De Jesus

- rdejesus@deloitte.com
- 408-704-2319



Presentation Objectives

- Describe Information Security and Privacy Policy Structure
- Elicit Feedback Through Interactive Tool
- Describe Policy Development Process
- Demonstrate the Process with an Example



This is an Interactive Presentation

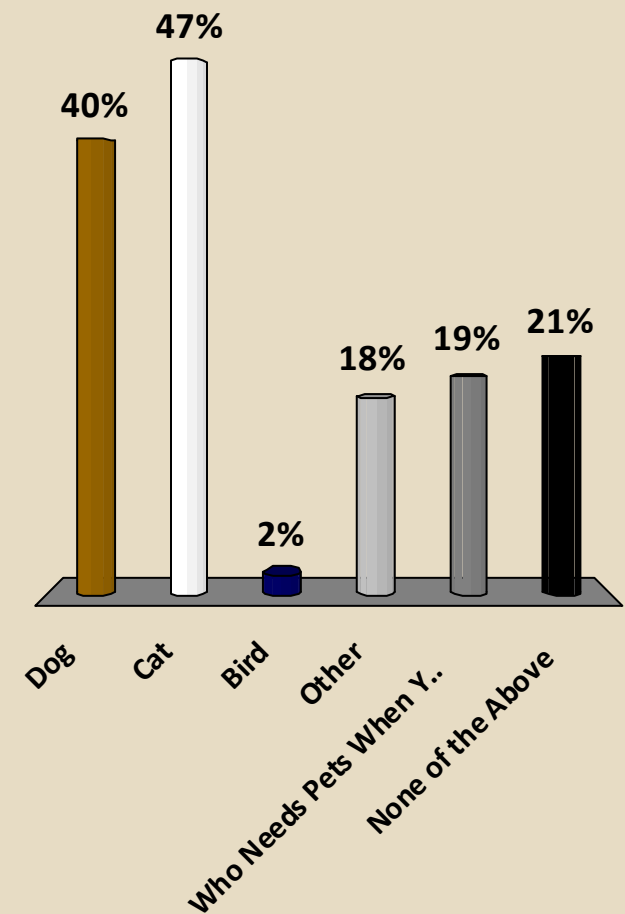
- ❑ Your Answers are Anonymous
- ❑ Press 1-10 (10=0 on keypad)
- ❑ Light On Keypad Will Turn Green If Success
- ❑ You Can Change Single Question Answers
- ❑ Results Will Be Displayed
- ❑ On Some Questions, You May Choose More Than One Answer if Indicated

Example:

Which Pets Do You Own?

Choose
All
That Apply

1. Dog
2. Cat
3. Bird
4. Other
5. Who Needs Pets When You Have Kids?
6. None of the Above

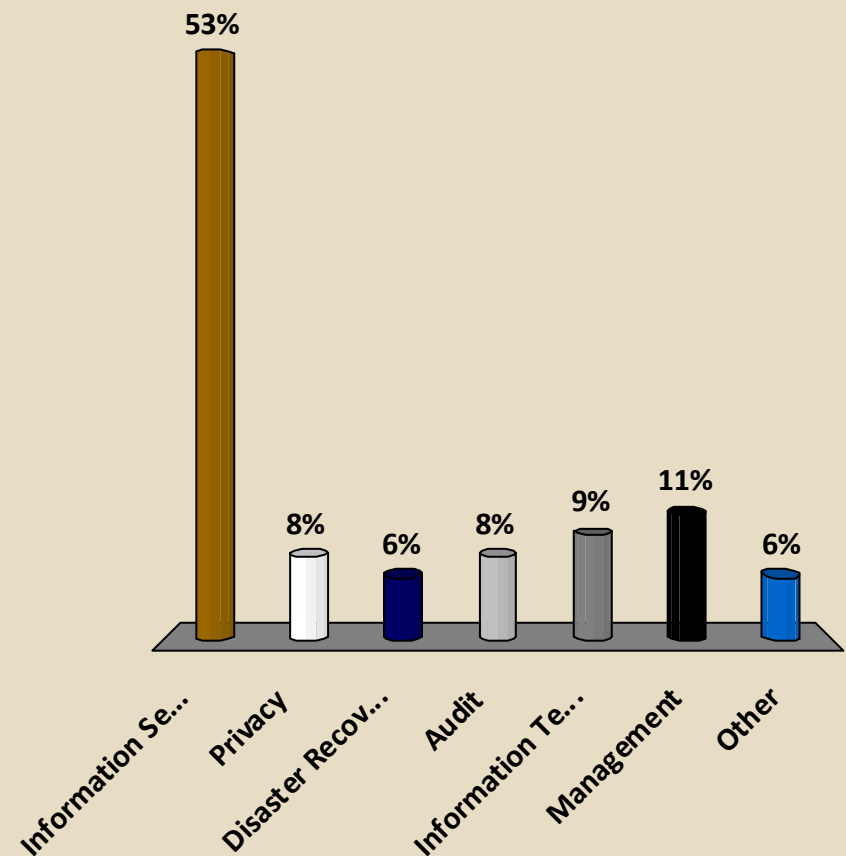


Which Is Your Primary Role? (What You Do Primarily)

Choose

1

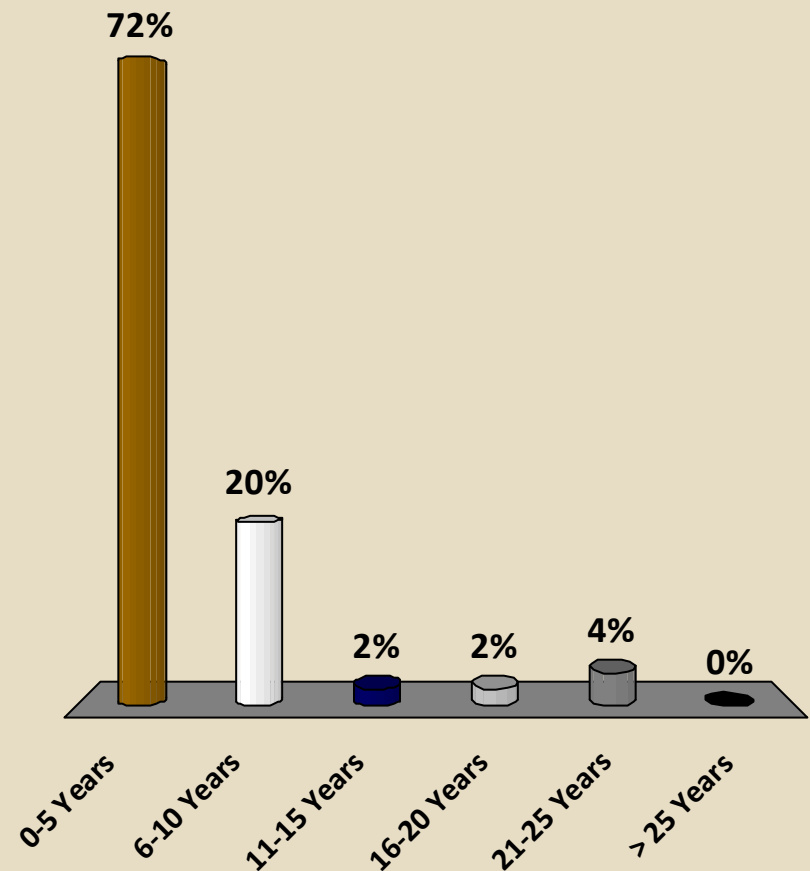
1. Information Security
2. Privacy
3. Disaster Recovery
4. Audit
5. Information Technology Professional
6. Management
7. Other



How Long Have You Been in the Current Role from Last Answer?

Choose
1

1. 0-5 Years
2. 6-10 Years
3. 11-15 Years
4. 16-20 Years
5. 21-25 Years
6. > 25 Years

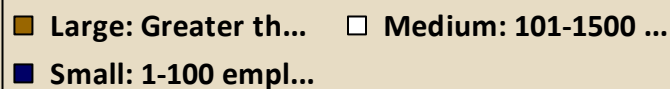
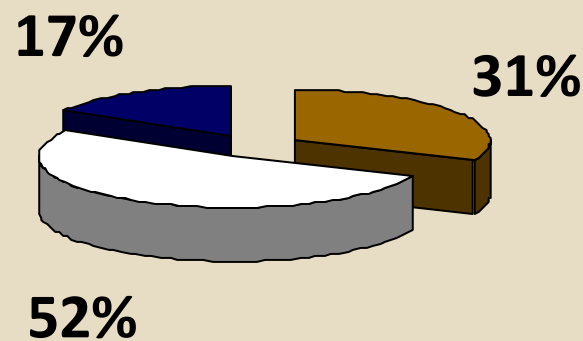


Choose

1

What Size Is Your Agency?

1. Large: Greater than 1500 employees
2. Medium: 101-1500 employees
3. Small: 1-100 employees





Policy Project Overview

- Goal of Policy Project
 - Develop new and revise existing policies to address the current and future landscape of information security and privacy threats, risks, and vulnerabilities to the State
- Development of common terminology and framework for policies, standards, procedures and guidelines is one of the initial steps

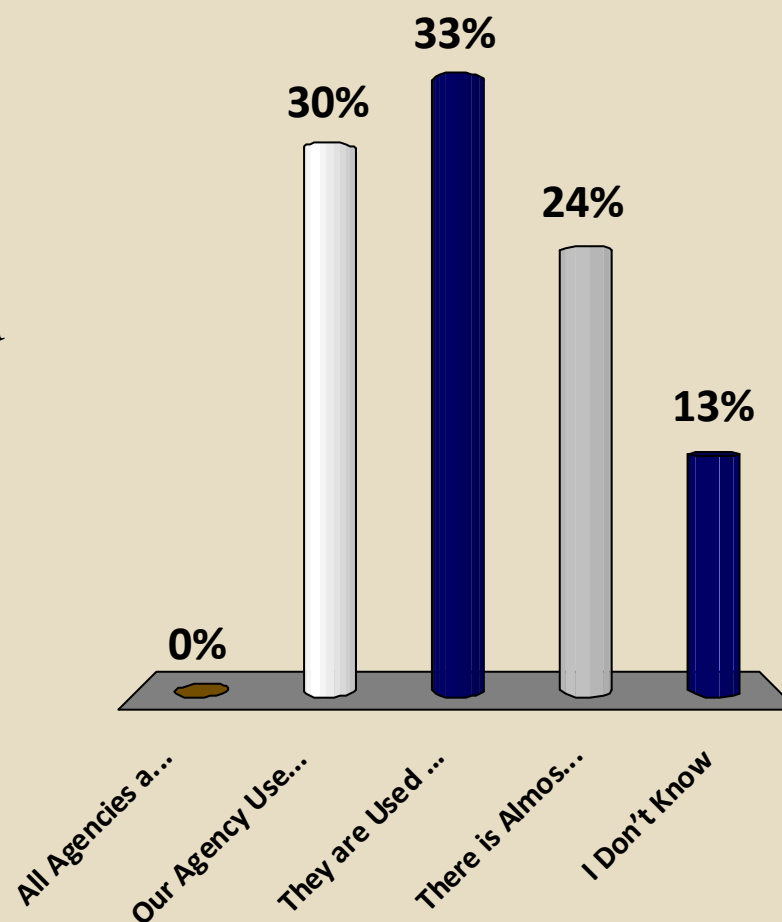
Policy Terminology and Framework


Defining **Policy**, **Standard**, **Procedure** and **Guideline** in the Context of Information Security and Privacy

How are Terms **Policy**, **Standard**, **Procedure**, and **Guideline** Used in the Enterprise and Agencies?

Choose
1

1. All Agencies and Enterprise Use These Terms to Describe the Same Thing in the Same Way
2. Our Agency Uses the Terms Uniformly, but They Are Not Used Consistently Across Agencies
3. They are Used Somewhat Consistently in Certain Groups
4. There is Almost No Consistency to the Use of These Terms
5. I Don't Know





How “Policy” is Defined

A high-level statement that describes mandatory or prohibited actions, applicable to individuals who fall within the scope of the policy, which aim to protect State information assets.

□ Policy Characteristics

- Formalized high-level statements
- Modified infrequently
- Require compliance - Failure to comply results in consequences
- May be further defined by standards, procedures and guidelines



Effect of New Definition for Policy

- SAM Chapter 5300 will only contain:
 - Policy statements
 - References to detailed standards, procedures or guidelines
 - References to the authoritative sources
- Standards, procedures, guidelines will be available outside of SAM on “Go RIM”
- Policy will be applicable to individuals to administer, implement and follow



Example New Policy:

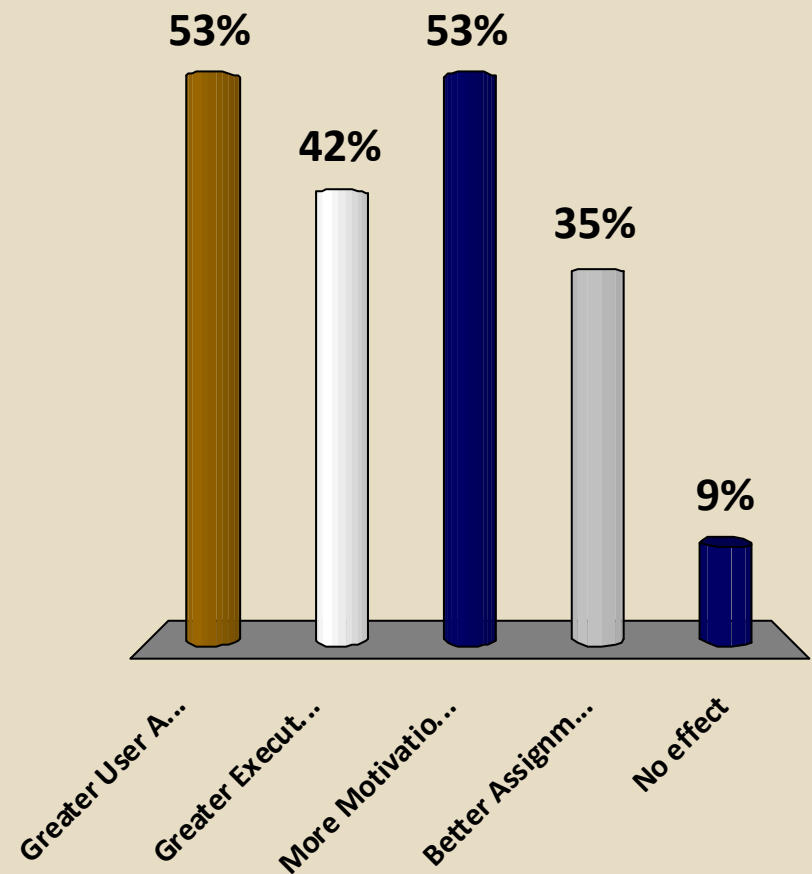
DATA OWNERSHIP

- Each **agency director** shall ensure that all assets are accounted for and have a designated owner. **Asset owners** with systems that process or contain data shall classify their assets in accordance with the Data Classification Standard.
- **Sources:** CobiT 4.0 - Level 1, 4.1, ISO/IEC 13335 (2004) Part 1, ISO/IEC 17799 (2005) Part 1, ISO/IEC 20000-2, NERC CIP-003-1: Security Management Controls, Security Guidelines for the Petroleum Industry - American Petroleum Institute

What Is The Likely Effect of Having Policy Statements Tied to Individuals?

Choose
All
That Apply

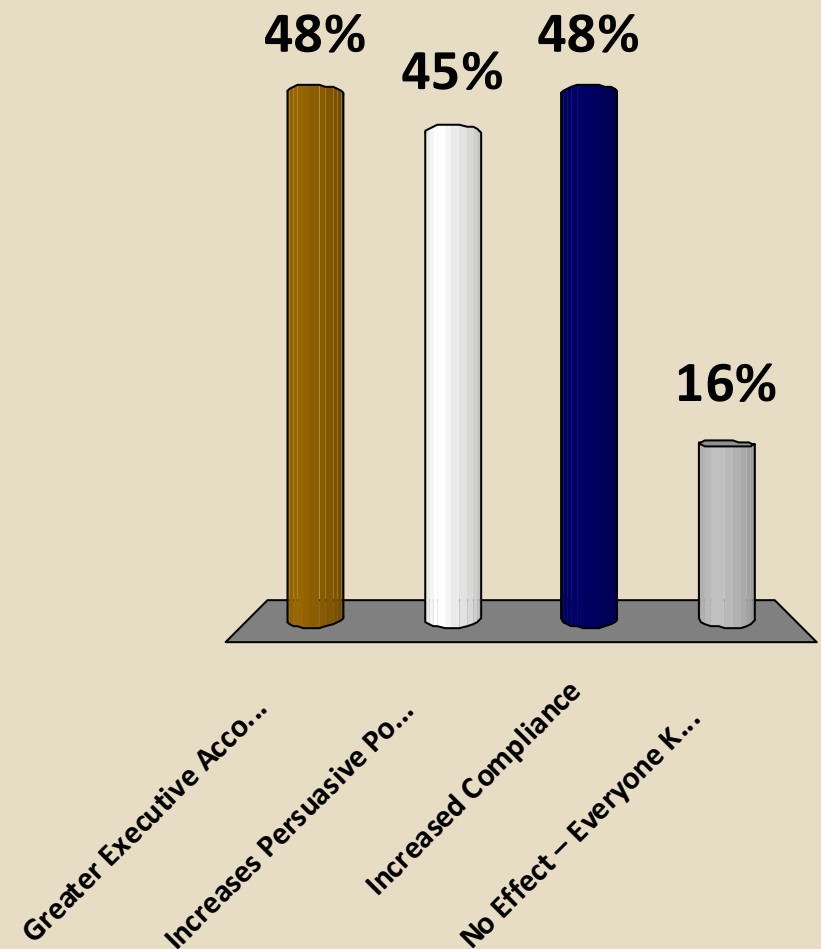
1. Greater User Accountability
2. Greater Executive Accountability
3. More Motivation Towards Compliance
4. Better Assignment of Ownership to Information Assets
5. No effect



What Is The Likely Effect of Clarifying that Policies are MANDATORY?

Choose
All
That Apply

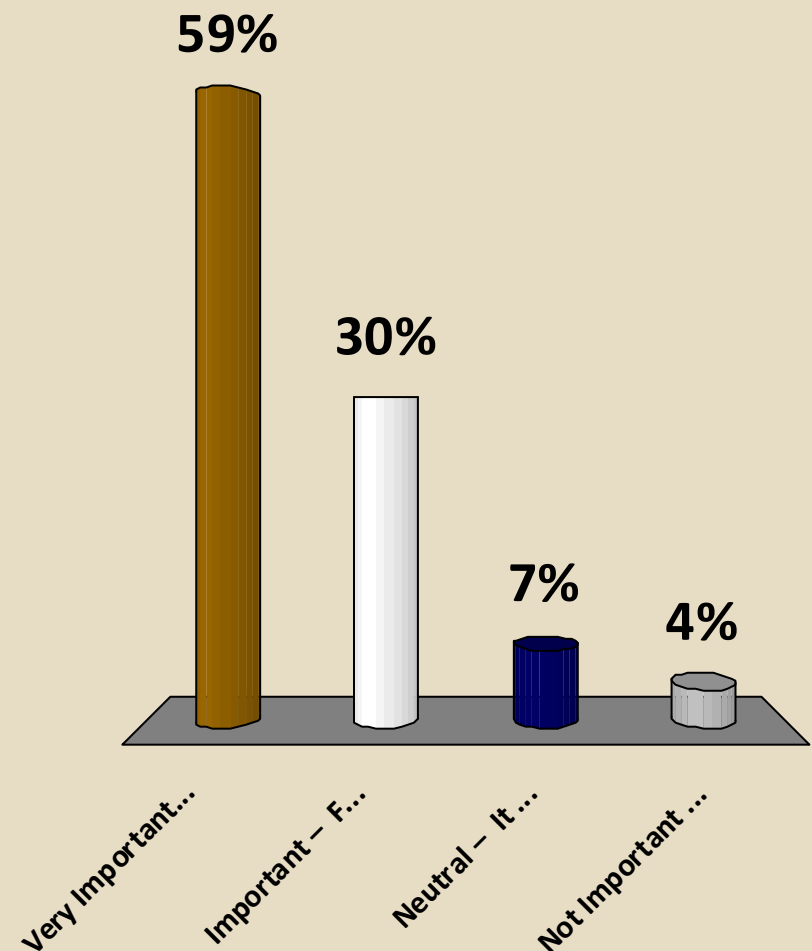
1. Greater Executive Accountability
2. Increases Persuasive Power of Agency ISOs
3. Increased Compliance
4. No Effect – Everyone Knows Policies Are Mandatory Now



How Important is it that Sources of the Policy Statements are Included in the Policy?

Choose
1

1. Very Important –
Helps to Enforce Policy
2. Important –
For Reference Purposes
3. Neutral –
It Doesn't Matter that Sources
are Identified
4. Not Important –
Should be Omitted to Avoid
Confusion





How “Standard” is Defined

A detailed published specification that contains measurable, mandatory rules to be applied to a process, technology, and/or action in support of a policy.

□ Standard Characteristics

- **Mandatory** – designed to support and conform to policy
- **Includes** accepted specifications for hardware, software, process, data, action or behavior
- **Modified** as frequently as required



Effect of New Definition of Standard

- Standards will target specific issues such as enterprise encryption, secure configurations, or wireless networking
- Agencies are encouraged to
 - Augment enterprise (state) standards
 - Develop agency-specific standards where OISPP has not addressed the topic



Example Standard

□ Data Classification Standard

- This standard shall be used by all agencies to classify all information and information systems collected or maintained by or on behalf of each agency based on the security objectives and potential impact on organizations and individuals.

. . .

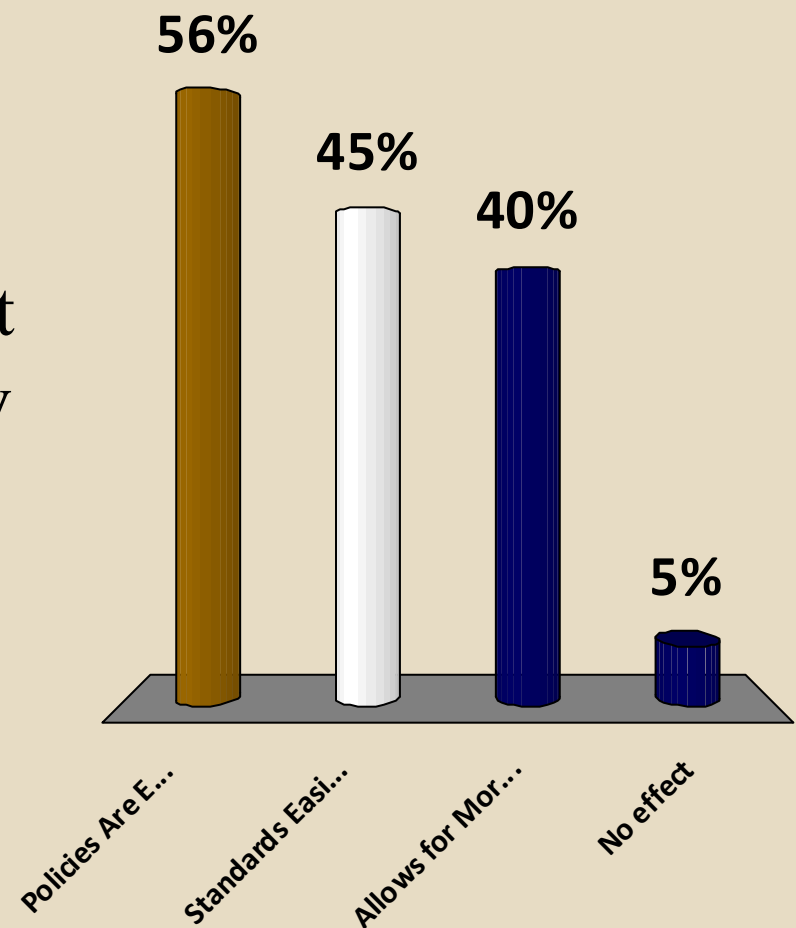
Asset owners shall recertify ownership and classification annually in accordance with the Annual Asset Ownership Certification Procedure.

- Source: FIPS-199

What is the Likely Effect of Having Standards Separate from Policies?

Choose
All
That Apply

1. Policies Are Easier to Understand by Keeping Statements Simple
2. Standards Easier to Interpret Because They Address Only One Topic
3. Allows for More Frequent Update to Standards
4. No effect

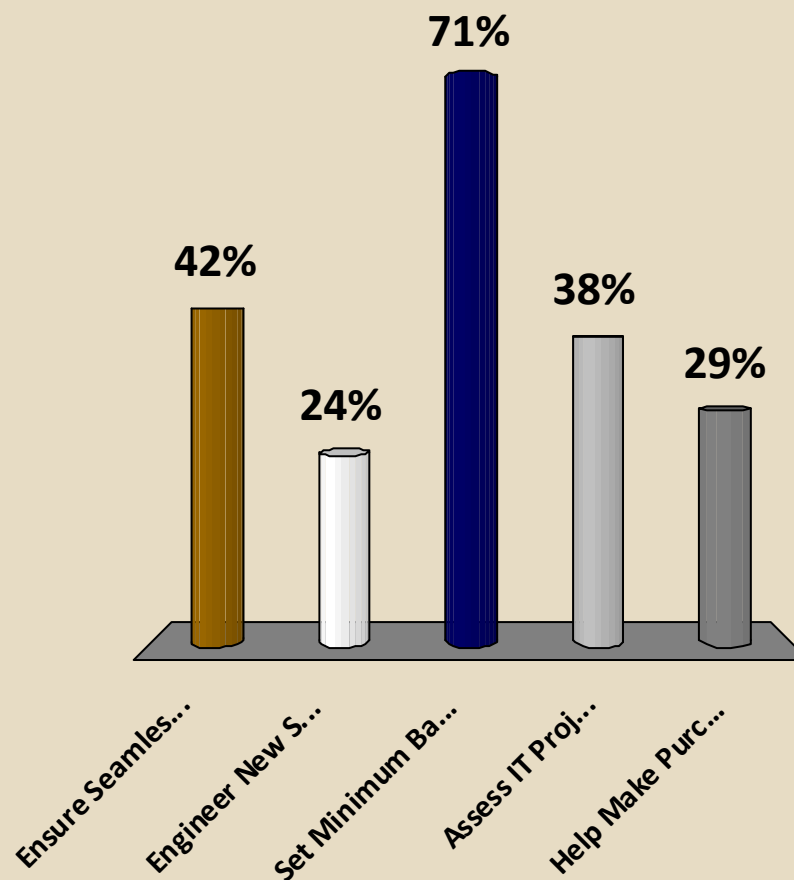


Why are Enterprise Standards Important to Your Agency?

Choose
All
That Apply

I Need These To:

1. Ensure Seamless Data Sharing between Groups or Technologies
2. Engineer New Secure Solutions
3. Set Minimum Baseline for Agency-Specific Standards
4. Assess IT Projects or Infrastructure
5. Help Make Purchasing Decisions





How “Procedure” is Defined

A specific series of actions an individual must take in order to comply with policies and standards.

□ Procedure Characteristics

- **Mandatory**
- **Detailed step-by-step instructions**
- **May provide a reference in times of crisis**



Effect of New Definition for Procedure

- Procedures such as the Enterprise Incident Management Procedure will be removed from SAM
- Procedures can and should be augmented with agency specific procedures when necessary



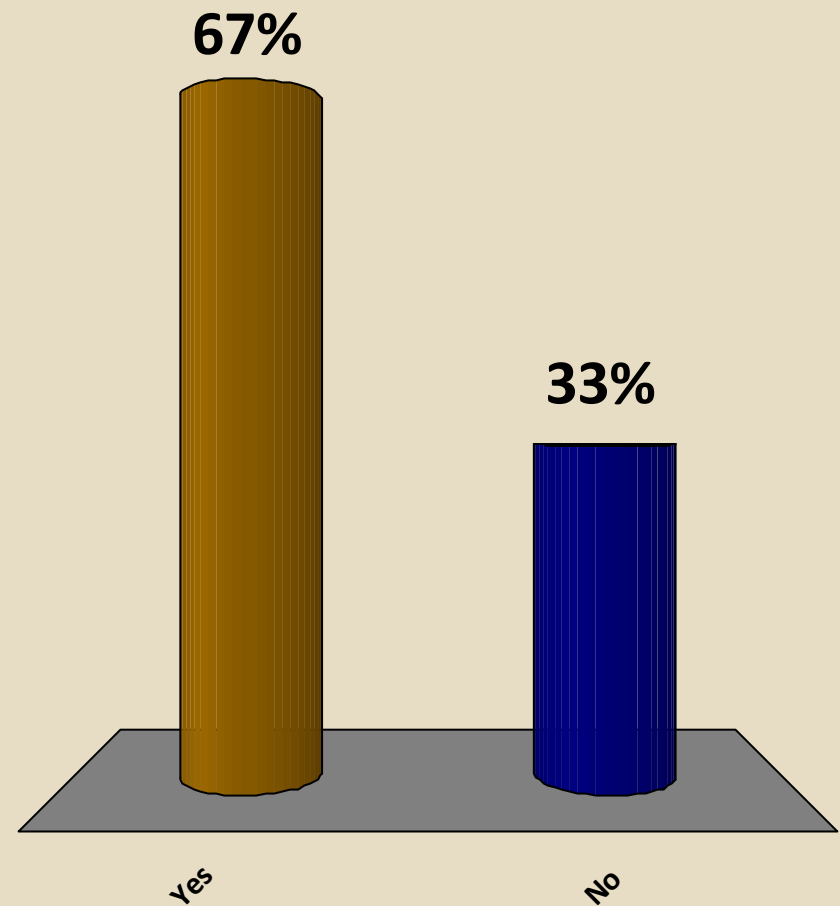
Example Procedure

- Annual Asset Ownership Certification Procedure
 - Before the close of each agency fiscal year, an asset owner shall:
 1. Physically verify that each asset is physically present,
 2. Verify that administrators and users with access are appropriate for each asset,
.....
 - Source: OISPP
 - See Asset Tracking Systems Guideline for recommendations on asset tracking systems

Does Your Agency Generally Have Procedures Separated from Policies?

Choose
1

1. Yes
2. No





How “Guideline” is Defined

Recommended actions that describe leading practices which support policies, standards and procedures.

□ Guideline Characteristics

- Not mandatory – rather, a suggestion of a leading industry practice
- Can change frequently based on environment or developments
- Can be used as a pre-cursor for what will eventually become a policy or standard



Effect of New Definition of Guideline

- Based on guidelines provided by OISPP, ISOs can provide answers regarding implementation of policies and standards, or other topics
- Document type represents a clear delineation between what is required (Policies, Standards, Procedures) and what is provided as recommendations (Guidelines)
- Agencies can develop standards built upon OISPP guidelines and standards, if they wish

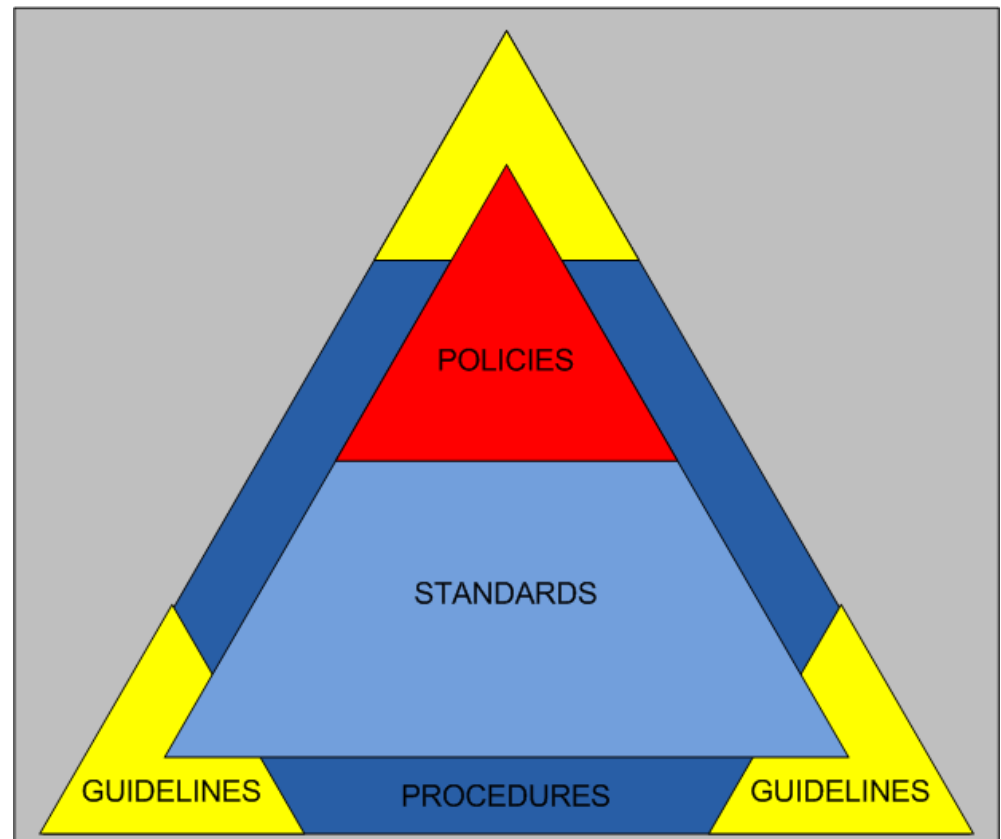


Example Guideline

- Asset Tracking Systems Guideline
 - Commercial asset tracking systems have been deployed in 103 agencies. Based on experience with those deployments, the following considerations should be given to choosing and deploying these systems:
 1. Investigate system capabilities for interconnections to vulnerability management systems
 2. . . .
 - Source: OISPP

How They Fit Together

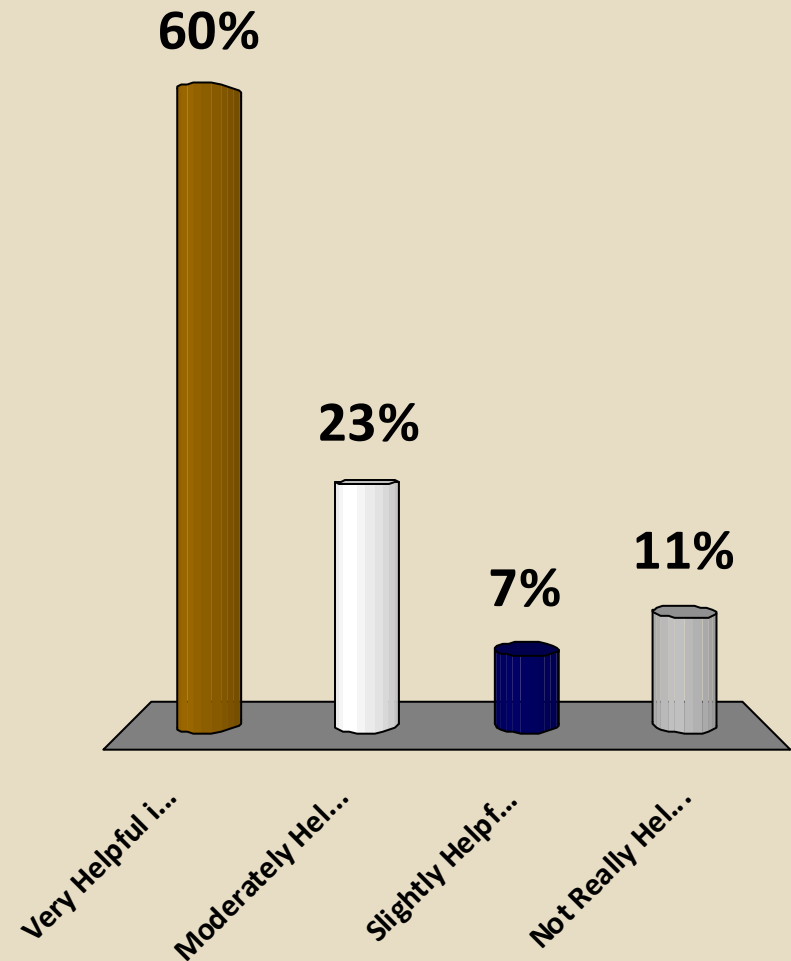
- Policies describe WHAT required actions to take from a HIGH-LEVEL
- Standards describe WHAT the DETAILED –LEVEL baseline requirements are for various technologies and configurations that are supported in the enterprise.
- Procedures may support both policies and standards and describe HOW to perform compliance activities.
- Guidelines may also support policies and standards, but are recommended leading practices on what to consider or HOW to perform security activities.



Effect of New Definitions in the Policy Framework on Your Jobs?

Choose
1

1. Very Helpful in Making Me More Effective in Protecting State Information Assets
2. Moderately Helpful
3. Slightly Helpful
4. Not Really Helpful at All

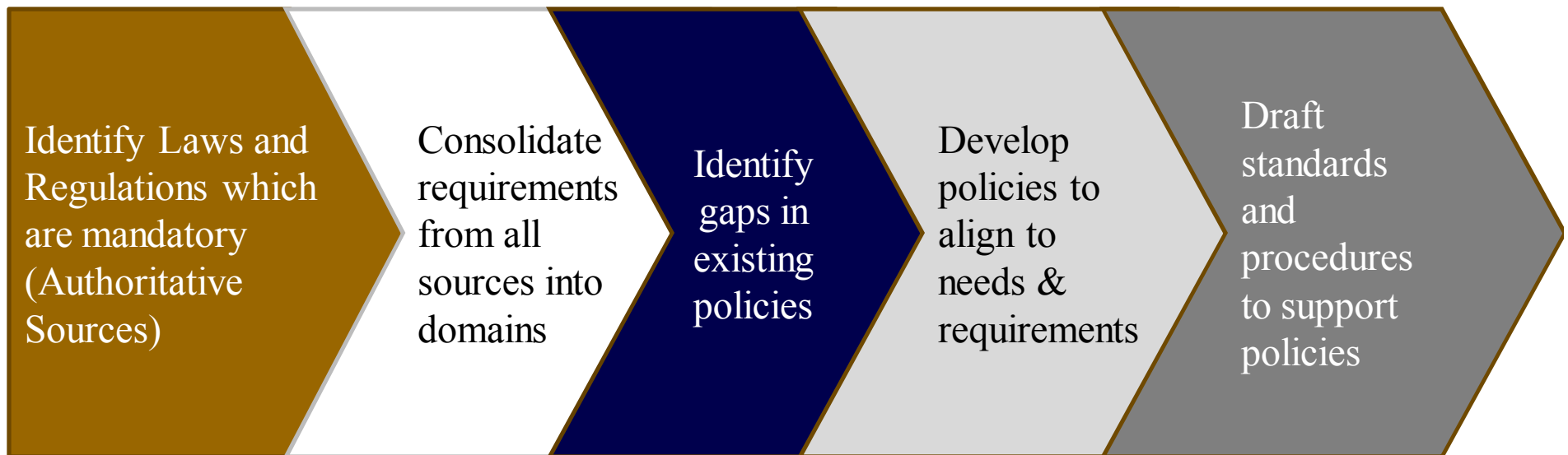




Policy Development Process

Policy Development Process

- Five Step Process to Develop Applicable Policies for State



Example of First Step in Process

□ Privacy Example

Identify Laws and Regulations which are mandatory (Authoritative Sources)



Authoritative Sources

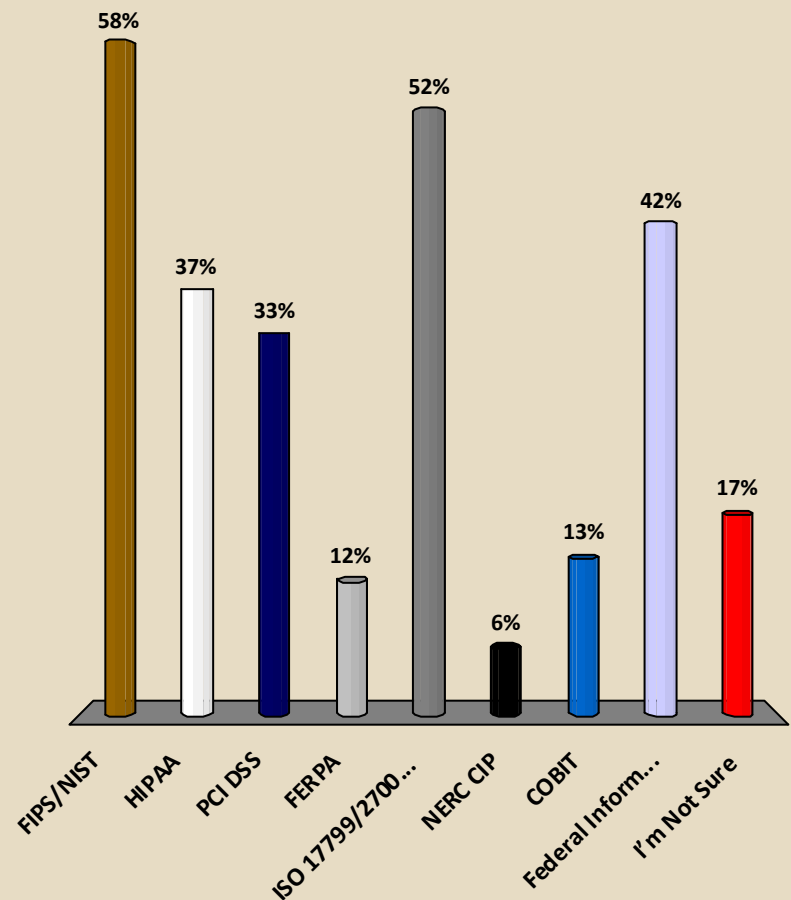
- California Information Practices Act
- California Government Code
- California Civil Code
- State Breach Notification Laws

Identify Laws
and Regulations
which are
mandatory
(Authoritative
Sources)

Which Security Authoritative Sources Apply to Your Agency?

Choose
All
That Apply

1. FIPS/NIST
2. HIPAA
3. PCI DSS
4. FERPA
5. ISO 17799/27002
6. NERC CIP
7. COBIT
8. Federal Information Security Management Act (FISMA)
9. I'm Not Sure

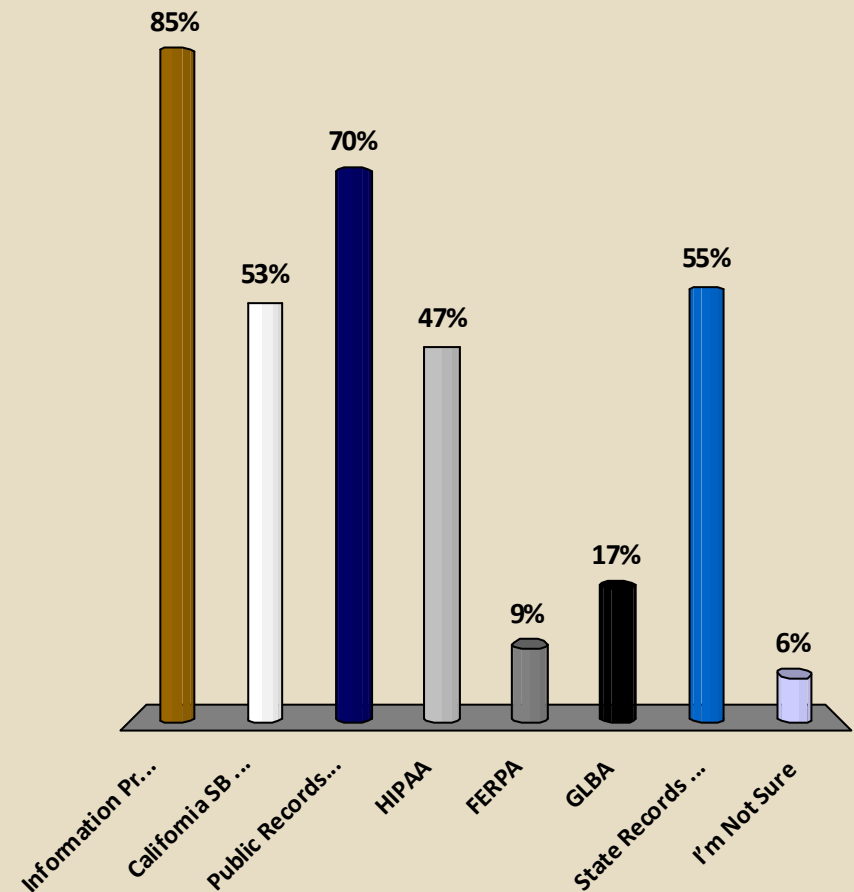


Identify Laws
and Regulations
which are
mandatory
(Authoritative
Sources)

Which Privacy Authoritative Sources Apply to Your Agency?

Choose
All
That Apply

1. Information Practices Act
2. California SB 1386
(Breach Notification)
3. Public Records Act
4. HIPAA
5. FERPA
6. GLBA
7. State Records Mgmt Act
8. I'm Not Sure



Consolidate
requirements
from all
sources into
domains

Hypothetical Example of Second Step in Process

Government Code Section 11015.5

(Distribution/sale of electronically collected PII)

A state agency shall discard without reuse or distribution any electronically collected personal information upon request by the user.



Government Code Sections 14755 (State Records Management Act)

No record shall be destroyed unless the director determines that the record has no value



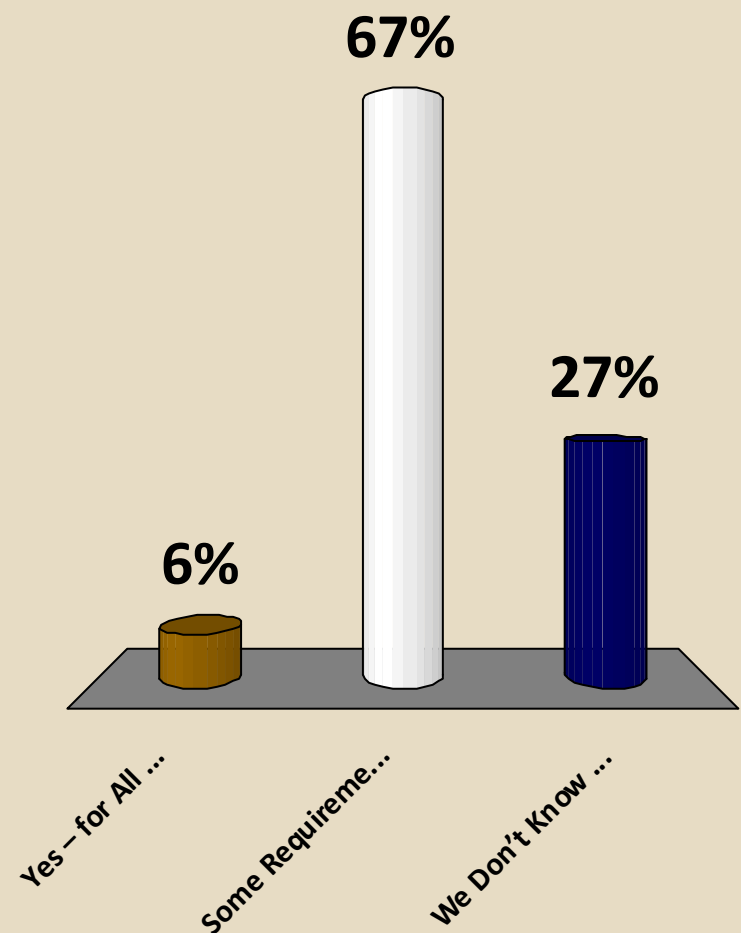
Consolidated Requirement Example:

No record shall be destroyed unless the director determines that the record has no value except for electronically collected personal information which shall be discarded upon user request.

Has Your Agency Consolidated Applicable Requirements into Your Policies?

Choose
1

1. Yes – for All Applicable Requirements
2. Some Requirements Have Been Consolidated
3. We Don't Know What Requirements Apply to Us



Consolidate
requirements
from all
sources into
domains

Example of Second Step in Process

Consolidated Requirement Example:
No record shall be destroyed unless the director determines that the record has no value except for electronically collected personal information which shall be discarded upon user request.

**Fits
Here**

Privacy Domains (Based on Fair Information Practices Principles)

1. Openness
2. Purpose Specification
3. Collection Limitation
4. Use Limitation
5. Integrity
6. Individual Participation
7. Security Safeguards
8. Accountability

Identify
gaps in
existing
policies

Example of Third Step in Process

Consolidated Requirement Example:
No record shall be destroyed unless the director determines that the record has no value except for electronically collected personal information which shall be discarded upon user request.

Compare
Requirement
to Existing
Policy

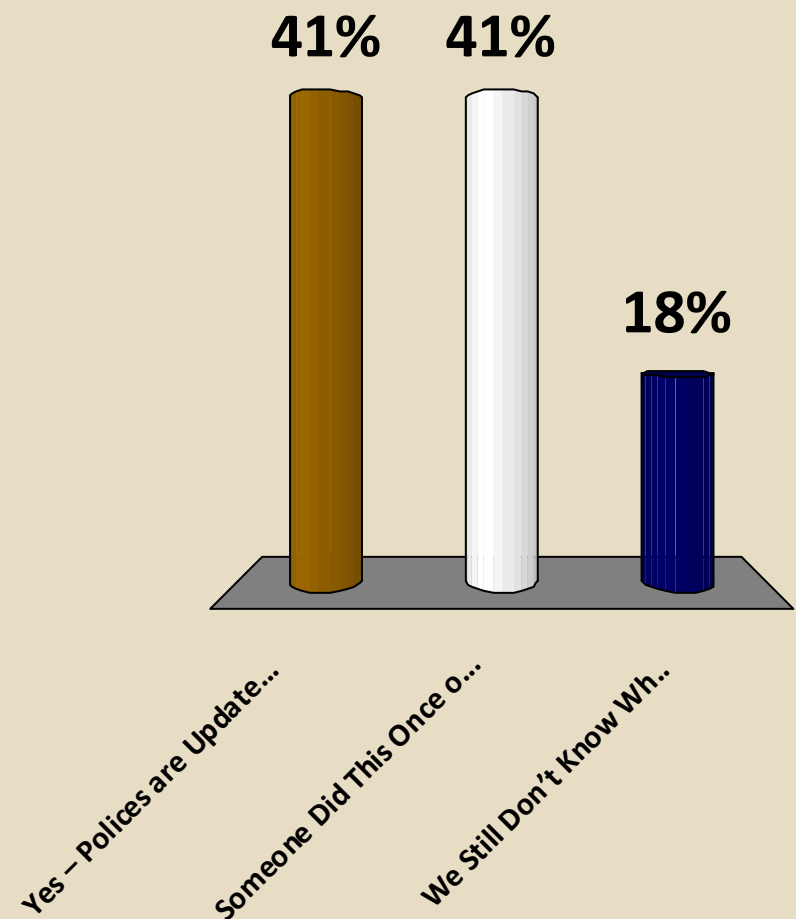
Requirement
Does Not Exist
in Policy

Gap
Identified

Has Your Agency Assessed Gaps in Your Policies Against Requirements?

Choose
1

1. Yes – Policies are Updated and Assessed Regularly
2. Someone Did This Once or It Is Partially Done
3. We Still Don't Know What Requirements Apply to Us



Fourth and Fifth Steps in Process

- Next Step is Actual Development

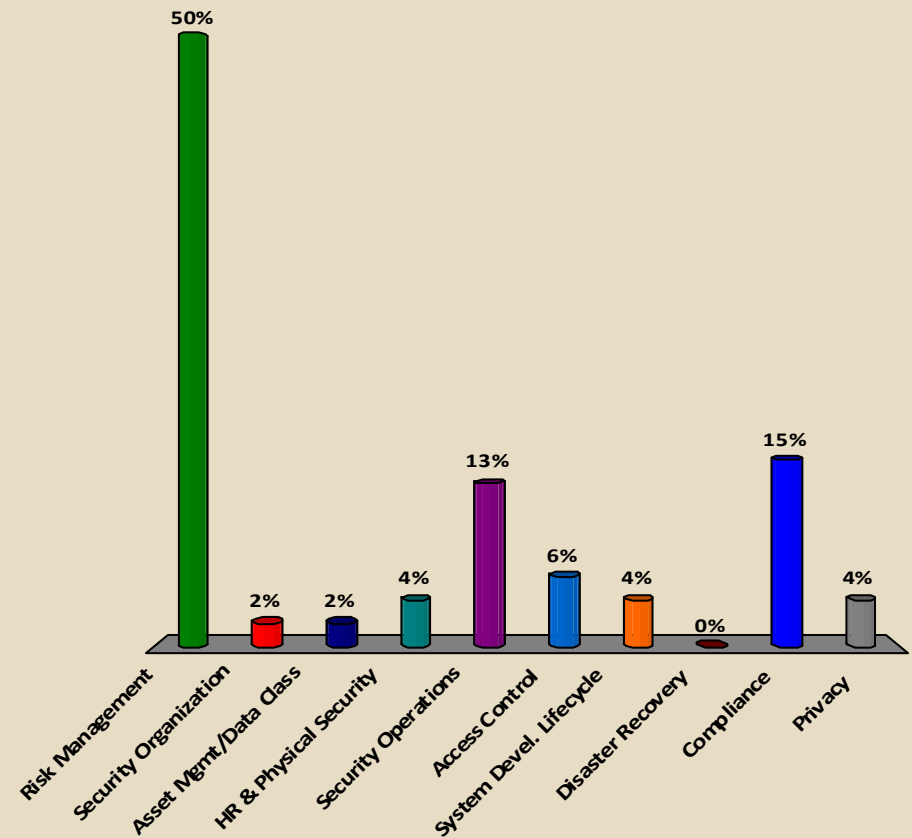


Issuing Which Policy Domain* is Your Highest Priority?

Choose
1

1. Risk Management
2. Security Organization
3. Asset Mgmt/Data Class
4. HR & Physical Security
5. Security Operations
6. Access Control
7. System Devel. Lifecycle
8. Disaster Recovery
9. Compliance
10. Privacy

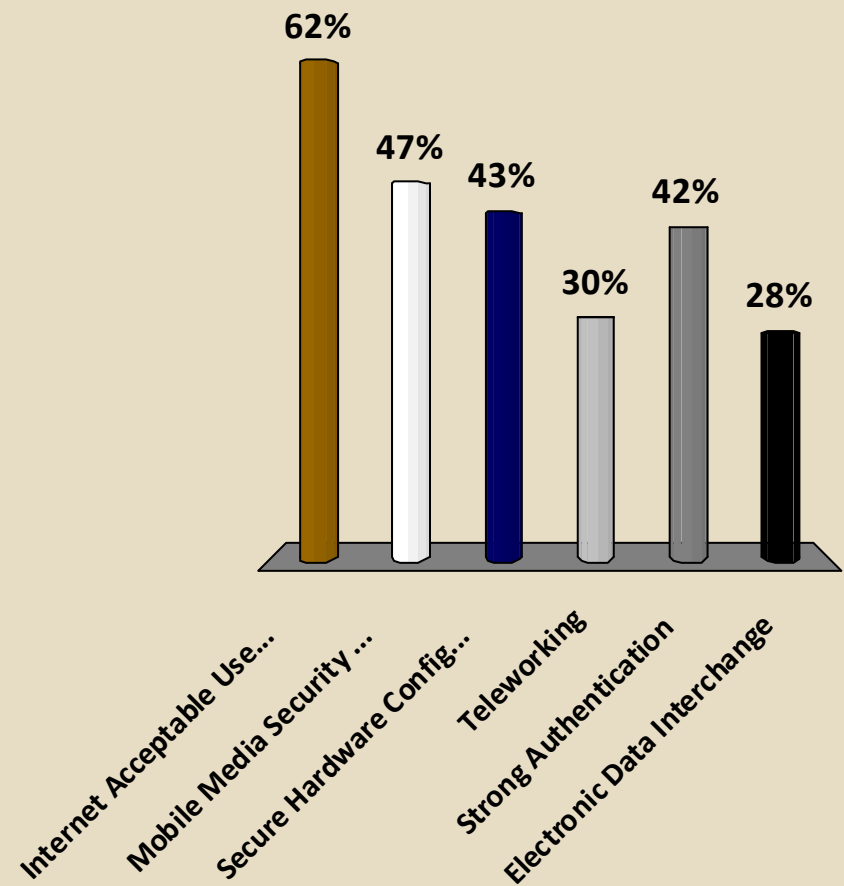
*Based on ISO Domains – Policy Mgmt not listed



Which Policy/Standard Topics are Current Priorities at Your Agency?

Choose
All
That Apply

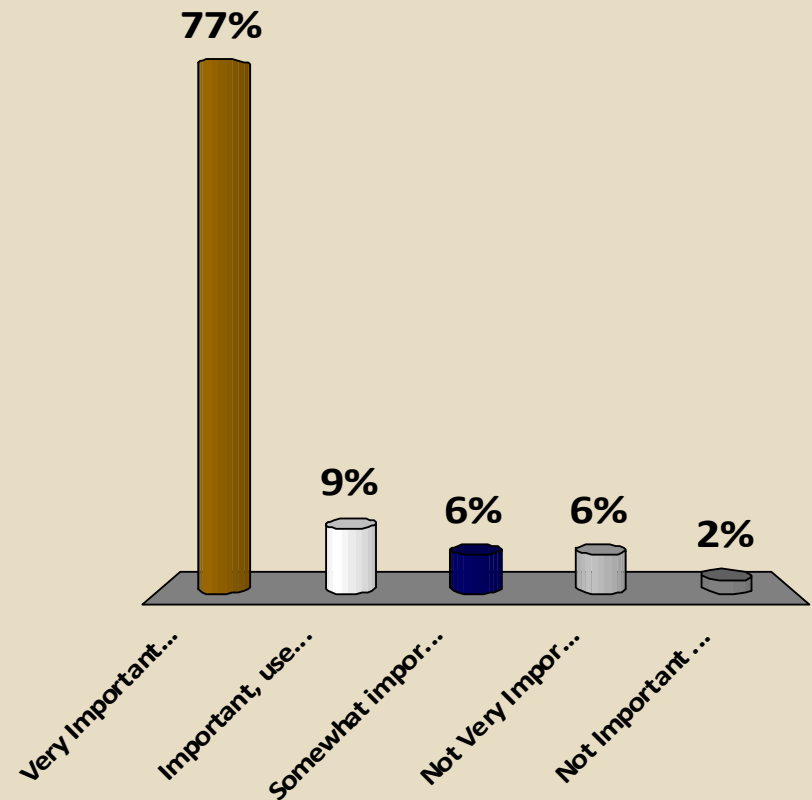
1. Internet Acceptable Use: Web 2.0, Peer-to-Peer networking
2. Mobile Media Security (USB drives, CD/DVDs, etc)
3. Secure Hardware Configurations
4. Teleworking
5. Strong Authentication
6. Electronic Data Interchange



Need for Information Security and Privacy Policies

Choose
1

1. Very Important - Wahoo!
I need this!
2. Important, useful but not critical
3. Somewhat important, but I'd rather OISPP was focused on my other needs
4. Not Very Important – we have few policy gaps
5. Not Important - we have sufficient policies

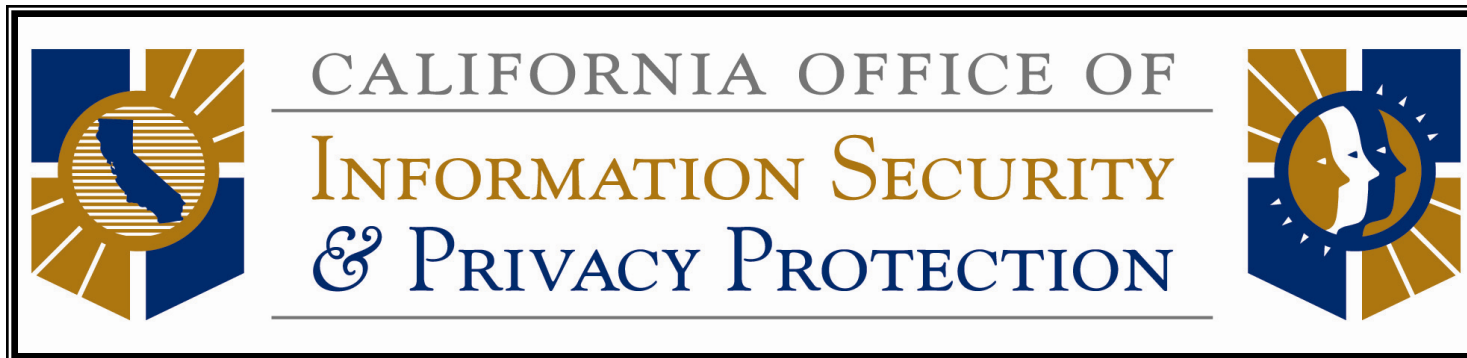




Next Steps / Contact Information

- Policy gap analysis and prioritization is currently in progress

- Contact OISPP for more information:
 - OISPP
 - security@oispp.ca.gov
 - (916) 445-5239



Deloitte.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

As used in this document, "Deloitte" means Deloitte & Touche LLP and Deloitte Consulting LLP, which are separate subsidiaries of Deloitte LLP.

Copyright © 2009 Deloitte Development LLC. All rights reserved.

Member of
Deloitte Touche Tohmatsu